AT-NO: JP409193577A

DOCUMENT-IDENTIFIER: JP 09193577 A

TITLE: IC CARD, INFORMATION PROCESSING TERMINAL AND INFORMATION COMMUNICATING SYSTEM

PUBN-DATE: July 29, 1997

INVENTOR-INFORMATION:
NAME
HOSHIKAWA, TOMOYUKI
IEGI, TOSHIATSU
MORIMOTO, TOSHIHIKO
KATO, KIMIHIRO

ASSIGNEE-INFORMATION:
NAME COUNTRY
N T T DATA TSUSHIN KK N/A

APPL-NO: JP08004371

APPL-DATE: January 12, 1996

INT-CL (IPC): B42D015/10, G06F015/00

ABSTRACT:

PROBLEM TO BE SOLVED: To provide an information communicating system, detecting unfairness when the unfairness is effected through an IC card and restraining the damages by effecting the control process of countermeasure quickly.

SOLUTION: In an information communicating system, wherein a host 11 at the side of a center is connected to a terminal 41 through a communication circuit 21 and an IC card 51 is utilized at the terminal 41, a process can be changed in accordance with the developing rate of abnormal phenomena, connecting

conditions and the like based on a crisis control table 113a accommodated in the terminal 41 to prevent the unfairness. When a phenomenon, which can not be decided definitely that it is unfairness, has occurred or when connection to the center has been disconnected, the countermeasures are employed to restrain the damage due to the unfairness. On the other hand, the generating condition of abnormal phenomena, which is detected in the terminal 41 or the IC card 51, is recorded and is collected in the host 11 of center side whereby the condition of abnormal phenomena in the whole of the system can be grasped. Further, countermeasure control process with respect to a newly detected unfairness can be effected quickly by deflecting the countermeasure to the crisis control table.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

**特開平9－193577**

(43)公開日　平成９年(1997)７月29日

| (51)Int.Cl.[6] | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|
| Ｂ４２Ｄ　15/10 | | | Ｂ４２Ｄ　15/10 | | |
| Ｇ０６Ｆ　15/00 | ３３０ | | Ｇ０６Ｆ　15/00 | ３３０Ｇ | |

審査請求　未請求　請求項の数７　ＯＬ　（全 12 頁）

(21)出願番号　特願平8－4371

(22)出願日　平成８年(1996)１月12日

(71)出願人　000102728
エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目３番３号

(72)発明者　星川　知之
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　家木　俊温
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　森本　俊彦
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(74)代理人　弁理士　鈴木　正剛

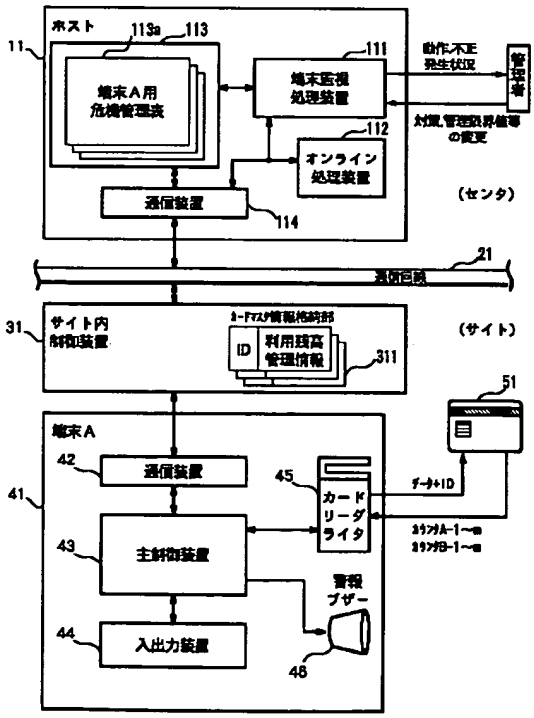
最終頁に続く

(54)【発明の名称】　ＩＣカード、情報処理端末、および情報通信システム

(57)【要約】

【課題】　ＩＣカードを通じて不正が行われた場合に、不正を検知して、速やかに対策制御処理をとって被害を抑える情報通信システムを提供する。

【解決手段】　通信回線２１を通じてセンタ側のホスト１１と端末４１が接続され、端末４１でＩＣカード５１を利用する情報通信システムにおいて、端末４１に内蔵された危機管理表１１３ａに基づき、異常現象の出現率や接続状況等に応じて処理を変更することで不正を防止し、不正であると確定できない現象が起こった場合や、センタとの接続が切れた場合についても対策をとり、不正による被害を抑える。また、端末４１およびＩＣカード５１で検知した異常現象の発生状況を記録し、センタ側のホスト１１で収集することで、システム全体における異常現象の状況を把握する。また、その対策を危機管理表４３３ａに反映することで、新たに検知した不正に対して速やかに対策制御処理を施す。



1

【特許請求の範囲】

【請求項１】　情報処理端末との間で電文の送受を行うＩＣカードであって、

前記情報処理端末から送られる電文が正常か否かを判定する手段と、

前記電文が異常で且つ該異常原因が不正操作によると判定した場合に、操作者が判らないような見せかけの偽電文を前記判定の度に生成して前記情報処理端末に返信する手段と、

前記生成した偽電文の返信情報を蓄積する手段と、

を有することを特徴とするＩＣカード。

【請求項２】　情報処理端末との間で電文の送受を行うＩＣカードであって、

前記情報処理端末から送られる電文が正常か否かを判定する手段と、

前記電文が異常で且つ該異常原因が不明な場合に、その旨を表す対応電文を生成して前記情報処理端末に返信する手段と、

前記生成した対応電文の返信情報を蓄積する手段と、

を有することを特徴とするＩＣカード。

【請求項３】　装着されるＩＣカードとの間で電文の送受を行う手段と、

前記ＩＣカードから送られる電文が正常か否かを判定する手段と、

前記電文が異常で且つ前記ＩＣカードに対する不正操作ないし不正操作の可能性があると判定した場合に、前記ＩＣカードに正常時と異なる電文を生成して返信する手段と、

前記生成した電文の返信情報を蓄積する手段と、

を有することを特徴とする情報処理端末。

【請求項４】　請求項１記載のＩＣカードに蓄積された偽電文の返信情報と請求項２記載のＩＣカードに蓄積された対応電文の返信情報の少なくとも一方を取得する手段と、

前記自端末に蓄積した返信情報または前記ＩＣカードより取得した返信情報から前記ＩＣカードを通じて行われた不正操作ないし不正操作の可能性を検知する不正検知手段と、

この不正検知手段が不正操作ないし不正操作の可能性を検知したときに予め検知内容毎に定めた対策制御処理を実行する不正対策処理手段と、

を有することを特徴とする請求項３記載の情報処理端末。

【請求項５】　前記不正対策処理手段は、前記不正検知手段の検知状況に応じて前記対策制御処理の内容を動的に更新することを特徴とする請求項４記載の情報処理端末。

【請求項６】　上位情報処理端末（以下、上位装置）と、オンラインまたはオフラインで前記上位装置に接続される下位情報処理端末（以下、下位装置）と、前記下

2

位装置との間で電文の送受を行うＩＣカードとから成る情報通信システムにおいて、

前記下位装置に、

前記ＩＣカードのアクセスに起因する異常現象の出現率と該ＩＣカードのアクセス状況とを含む監視情報を蓄積する手段を備えるとともに、

前記上位装置に、

前記下位装置から前記監視情報を取得する手段と、

前記取得した監視情報に基づき前記ＩＣカードまたは下位装置に対する不正操作ないし不正操作の可能性を検知する不正検知手段と、

前記不正検出手段が不正操作ないし不正操作の可能性を検知したときに予め不正内容毎に定めた対策制御処理を実行する不正対策処理手段と、

を備えたことを特徴とする情報通信システム。

【請求項７】　前記不正対策処理手段は、前記不正検知手段で検知した検知状況に応じて前記対策制御処理の内容を動的に更新することを特徴とする請求項６記載の情報通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＣカードを利用した情報通信システムに係り、特にＩＣカードを通じて行われる不正操作への対策制御技術に関する。

【０００２】

【従来の技術】従来より、ネットワークにより上位情報処理端末（上位装置、以下、センタと称する）と下位情報処理端末（下位装置、以下、単に端末と称する）とを接続して情報の授受を行う情報通信システムが、種々の産業界において開発され、利用されている。一般に、この種の情報通信システムでは、センタから多数の端末の動作を常時監視あるいは制御するオンライン方式と、センタと端末との間で、監視項目のデータ，監視結果，評価データ等の監視情報、あるいは監視プログラムを定期的に授受することで、基本的に端末側だけで動作の監視あるいは制御するオフライン方式とが採用されている。このような情報通信システムにおいては、運用上のセキュリティの確保や、不正操作に対する管理体制の強化が重要な課題となっている。この対応策として、従来よりＩＣカードの利用が有効であると考えられている。すなわち、ＩＣカードにユーザＩＤ情報や暗号鍵等の送受信機能を持たせ、このＩＣカードを端末に装着したときにユーザＩＤ情報等の認証を行い、正当であることが確認できたときにのみシステムの利用を可能とする。

【０００３】

【発明が解決しようとする課題】上記のようにＩＣカードを利用する情報通信システムにおいては、暗号化／復号化、認証手段などのセキュリティが施されているが、暗号鍵や認証手順などが知られてしまうと、容易に不正操作が行われてしまう。特に、オフラインの状態でＩＣ

カードに対して種々の不正操作の試みがなされ、ＩＣカード自身に改ざんが施された場合、ＩＣカードの認証を行う端末、あるいはこの端末に接続されたセンタ側では、不正操作の状況やＩＣカードのセキュリティがどこまで破られたかを知ることができない問題があった。

【０００４】また、センタ側で端末の監視を常時オンラインで行うか、時間や処理回数等を基準に定期的に監視情報を交換するようにして端末側でオフラインの状態で監視するかは、システム構築時にしか選択することができない。そのため、この種の情報通信システムでは、センタに設けられるホストコンピュータ（以下、ホスト）と端末との間の通信を減らして効率的に端末の動作監視を行ったり、ホストでのリアルタイムな動作監視を行ったりすることなどを、運用中に変更することができなかった。

【０００５】本発明の主たる課題は、ＩＣカードを用いた情報通信システムにおいて、オフラインで行われた不正操作の状況やＩＣカードのセキュリティが破られた過程を検知することができ、不正操作を検知したときは速やかに対策制御処理を行って、不正操作に起因する被害を最小限に抑える技術を提供することにある。本発明の他の課題は、ＩＣカードを利用する端末とホストとを結んで構成される情報通信システムにおいて、稼働状況に応じて端末の運用形態をリアルタイムに変更できるようにすることにある。

【０００６】

【課題を解決するための手段】上記の主たる課題を解決するため、本発明は、まず、不正操作ないし不正操作の可能性を検知し得る機能を備えたＩＣカードを提供する。第１構成のＩＣカードは、情報処理端末から送られる電文が正常か否かを判定する手段と、前記電文が異常で且つ該異常が不正操作に基づくと判定した場合に、操作者が判らないような見せかけの偽電文を前記判定の度に生成して前記情報処理端末に返信する手段と、前記生成した偽電文の返信情報を蓄積する手段と、を有することを特徴とする。

【０００７】また、第２構成のＩＣカードは、情報処理端末から送られる電文が正常か否かを判定する手段と、前記電文が異常で且つ該異常が不明の場合に、その旨を表す対応電文を生成して前記情報処理端末に返信する手段と、前記生成した対応電文の返信情報を蓄積する手段と、を有することを特徴とする。上記偽電文または対応電文を返信する場合、受信した情報処理端末側では直ちに必要な対策制御処理を行ってもよく、そのまま自端末の運用を継続させておいて、必要な時点で対策制御処理を行うようにしてもよい。

【０００８】本発明は、また、前述の情報通信システムの下位装置としての利用に適した情報処理端末を提供する。この情報処理端末は、装着されるＩＣカードとの間で電文の送受を行う手段と、前記ＩＣカードから送られる電文が正常か否かを判定する手段と、前記電文が異常で且つ前記ＩＣカードに対する不正操作ないし不正操作の可能性があると判定した場合に、前記ＩＣカードに正常時と異なる電文を生成して返信する手段と、前記生成した電文の返信情報を蓄積する手段と、を有することを特徴とする。



【０００９】他の形態の情報処理端末として、前記自端末に蓄積した返信情報または上記本発明のＩＣカードより取得した返信情報から前記ＩＣカードを通じて行われた不正操作ないし不正操作の可能性を検知する不正検知手段と、この不正検知手段が不正操作ないし不正操作の可能性を検知したときに予め検知内容毎に定めた対策制御処理を実行する不正対策処理手段と、を備える構成も可能である。このような構成において、不正対策処理手段は、前記不正検知手段で検知した不正の状況に応じて対策制御処理の内容を動的に更新することができるように構成することが好ましい。

【００１０】本発明は、さらに、ＩＣカードと情報処理端末とを利用した、改良された情報通信システムを提供する。この情報通信システムは、上位情報処理端末（上位装置）と、オンラインまたはオフラインで上位装置に接続される下位情報処理端末（下位装置）と、下位装置との間で電文の送受を行うＩＣカードとから成る。下位装置には、前記ＩＣカードのアクセスに起因する異常現象の出現率と該ＩＣカードのアクセス状況とを含む監視情報を蓄積する手段を備える。また、上位装置には、前記下位装置から前記監視情報を取得する手段と、前記取得した監視情報に基づき前記ＩＣカードまたは下位装置に対する不正操作ないし不正操作の可能性を検知する不正検知手段と、前記不正検出手段が不正操作ないし不正操作の可能性を検知したときに予め不正内容毎に定めた対策制御処理を実行する不正対策処理手段と、を備える。ここにいう監視情報とは、ＩＣカードのアクセスに起因して生じる、システムの安全性の程度を表す情報をいう。必要に応じて上述の各返信情報を含ませることができる。このような情報通信システムにおいて、前記不正検知手段は、前記ＩＣカードのアクセス時における異常現象の出現率と接続状況とを計測することで前記不正を検知し、前記不正対策処理手段は、前記不正検知手段で検知した不正の状況に応じて前記対策制御処理の内容を動的に更新するように構成することが好ましい。

【００１１】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を詳細に説明する。本発明の一実施形態による情報通信システムの全体構成例を図１に示す。図１を参照すると、上位装置として機能するセンタは、ホストコンピュータ（以下、単にホストと称する）１１を備えている。ホスト１１には、通信回線２１を通じて、複数のサイト（ビル、店舗などの単位の総称、以下同じ）内のサイト内制御装置３１が接続されている。各サイト内制

御装置３１には、ＬＡＮ（ローカルエリアネットワーク）等を通じて、多数の下位装置である端末（図１では端末Ａを代表して示す）４１が接続されている。端末４１は、ＩＣカード５１によってアクセス（データその他の情報の書込／読出、以下同じ）可能となっている。

【００１２】ホスト１１は、サイト内制御装置３１や各端末４１の動作、不正発生状況等を収集して管理者に知らせ、管理者からの指示により必要な対策、管理限界値等の変更等の処理を行う端末監視処理装置１１１と、ブラックリストの作成／参照、詳細なチェック機能、ホストキー照合等を行うオンライン処理装置１１２と、端末毎の動作，不正発生の内容や回数，それぞれの不正内容への対策制御処理，管理限界値をまとめた危機管理表１１３ａを格納する危機管理表格納部１１３と、サイト内制御装置３１や端末４１との通信を行うための通信装置１１４とを備えている。危機管理表１１３ａには、後述の端末４１の危機管理表４３３ａと対応した設定情報が格納されている。

【００１３】サイト内制御装置３１は、例えば電子現金情報を扱う場合のカードマスタ情報（ＩＤ、利用残高、その他の管理情報）を格納するカードマスタ情報格納部３１１や、カードマスタ情報の読み出し、あるいは書き込みを制御する手段（図示省略）が備えられている。

【００１４】端末４１は、サイト内制御装置３１やホスト１１と通信を行うための通信装置４２と、データの正当性確認、データ照合、取引傾向の集計、不正発生状況の集計、動作時間の測定のほか、ＩＣカード５１を通じて行われる不正操作その他の異常処理状態を検出して必要な対策制御処理を実行する主制御装置４３と、操作者が入力するデータを入力するとともに主制御装置４３の処理結果を出力する入出力装置４４と、ＩＣカード５１を離脱自在に装着するとともに、カード情報の読み書きを行うカードリーダライタ４５と、警報ブザー４６とを備えて構成される。

【００１５】図２に、主制御装置４３の詳細なブロック構成例を示す。主制御装置４３は、装置全体の制御を統括する主制御部４３１と、危機管理表格納部４３３に格納された危機管理表４３３ａに基づいて必要な対策制御処理を行う対策制御処理部４３２とを備えて、不正対策処理手段を実現している。危機管理表４３３ａは、対策制御処理部４３２が認識可能なテーブル形式の構造を有し、自端末についての不正発生の内容やその回数，各不正内容への対策制御処理，管理限界値とその統計値の情報が格納されている。

【００１６】主制御部４３１は、サイト内制御装置３１のカードマスタ情報格納部３１１との間で所要の情報を交換し合い、あるいはＩＣカード５１からのメモリ情報を読み取り、それにより得た情報を危機管理表４３３ａに書き込む。また、ホスト１１からの要求に応じて危機管理表４３３ａを更新する。この更新は、オンライン



中、あるいはオフラインのいずれの場合も可能になっている。つまり、実行中の対策制御処理の部分の更新が動的に可能になっている。対策制御処理の内容としては、例えばＩＣカード５１とホスト１１とを直接結ぶ完全オンライン処理の要求、統計値の報告要求、カードを排出しない、警告を鳴らす、データを受けない等の処理がある。対策制御処理部４３２は、統計値の報告要求の際には、各項目の統計値をホスト１１の端末監視処理装置１１１に送る。また、オンライン処理要求の際には、カードリーダライタ４５とホスト１１のオンライン処理装置１１２とを接続し、ＩＣカード５１との情報の授受がホスト１１により直接に制御されるようにする。

【００１７】主制御部４３１と対策制御処理部４３２には、デバイス管理部４３４を介して通信制御部４３５，カード制御部４３６，および警報制御部４３７が接続されている。デバイス管理部４３４は、対策制御処理部４３２が必要な処理を実行する際に、デバイスのアドレス割当等を行うものである。このアドレス割当等を受けて、通信制御部４３５は通信装置４２を制御し、カード制御部４３６はカードリーダライタ４５のカード装着／離脱機構やカード情報のアクセスを制御し、警報制御部４３７はカードリーダライタ４５，警報ブザー４６の制御を行う。

【００１８】主制御装置４３は、また、カウンタ処理部４３８、カウンタ格納部４３９、不正検知部４４０、および動作時間間隔等を計測するための時間計測部（タイマおよびその附属装置）４４１を備えている。カウンタ処理部４３８は、不正発生回数を集計する第１カウンタＡと，不正操作の可能性のある回数を集計する第２カウンタＢを備えており、それぞれのカウンタ値をカウンタ格納部４３９のテーブル４３９ｂに格納する。カウンタ格納部４３９は、例えばＥＥＰＲＯＭ（書換可能なＲＯＭ）で構成され、取引データがあるときはそれを格納する取引データ格納部４３９ａが形成される。なお、カウンタ格納部４３９は、ホスト１１が任意の時点でその内容を参照可能なように構成されている。

【００１９】不正検知部４４０は、ＩＣカード５１の正当性を確認するための認証処理部４４０ａと、不正検知に必要な演算処理を行う演算処理部４４０ｂとから構成されている。不正検知処理については後述する。

【００２０】以上の構成の端末４１において利用されるＩＣカード５１の詳細ブロック構成を図３に示す。この種のＩＣカードは、一般にＣＰＵ、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭを備えている。そこで、本実施形態は、図３に示すように、ＣＰＵ５１２に、通信制御部５１２ａ、実行制御部５１２ｂ、数値演算処理部５１２ｃを形成し、ＲＯＭ５１３に、処理プログラム格納部５１３ａ、カウンタ処理部５１３ｂ、認証処理部５１３ｃを形成する。カウンタ処理部５１３ｂは、不正発生回数を計測する第１カウンタＡ、および不正操作の可能性のある回数

を計測する第2カウンタBの機能を備えている。EEPROM514には、端末41が備えるものと同一内容のカウンタ格納部514を形成しておく。RAM515はワークエリア515aとして用いる。なお、CPU512には、外部インタフェース511が接続される。

【0021】本実施形態では、上記構成のICカード51を通じて端末41の不正操作ないし不正操作の可能性があることを検知する不正検知機能をICカード51自体にも持たせる。この不正検知機能の概要を、端末41との間で電文を送受信する場合の実行制御部512bでの処理手順例を示す図4、および電文の流れを示した図5にしたがって説明する。

【0022】図4を参照すると、まず、電文番号であるn＝1を設定して（ステップ（以下、S）1）、電文nの受信待ちとする（S2）。電文nが受信されたか否かを判断し（S3）、受信された場合には（S3：Yes）、第2カウンタB－(n-1) をカウントダウンして（S4）、誤り訂正符号をチェックする（S5）。誤り訂正符号が正しければ（S5：OK）、電文の正当性をチェックする（S6）。正当ならば（S6：OK）、正しいレスポンス電文nを作成し（S7）、そのレスポンス電文nを相手方に送信する（S8）。図5（a）はこの様子を示すものである。その後、その電文nについての通信が終了したか否かを判断し（S9）、通信終了ならば（S9：Yes）、そのまま処理を終了する。

【0023】上記S3の処理において、電文nが受信されない場合には（S3：No）、電文nの受信待ちがタイムアウトか否かを判断し（S10）、タイムアウトでなければ（S10：No）、S2の処理に戻り、タイムアウトであれば（S10：Yes）タイムアウトに対応した電文nを作成し（S11）、S8の処理に移行する。また、上記S5において、誤り訂正符号に誤りがあった場合には（S5：NG）、伝送エラーに対応した電文nを作成して（S12）、S8に移行する。図5（b），（d）は、この様子を示すものである。

【0024】一方、上記S6の処理において、電文nが正当でない場合には、第1カウンタA－nをカウントアップするとともに（S13）、操作者が判らないような見せかけの偽電文を作成して（S14）、S8に移行する。この偽電文は電文毎に異なるものとする。図5（c）は、この様子を示すものである。また、上記S9において、通信終了でない場合には（S9：No）、図5（d）に示すように第2カウンタB－nをカウントアップするとともに（S15）、電文番号をn＝n＋1として（S16）、S2の処理に戻る。

【0025】以上のように、上記S6の処理では、暗号化・復号化・電子署名を用いた認証技術、コマンド／レスポンスのフォーマットチェックなどにより電文の正当性をチェックする。そして、正当でないと判断した場合には第1カウンタAをカウントアップし、見せかけの偽電文を作成して送信する。正当な場合は正当なレスポンス電文を作成し、送信する。後続電文を受信する予定がある場合は、第2カウンタBをカウントアップしておいて、受信待ちする。次の電文を受信した場合は、カウンタBがカウントダウンして元に戻るが、不正や伝送エラーにより次の電文が待ち時間内に受信できなかった場合は、第2カウンタBはカウントアップされたままの状態となり、決められた伝送手順に従って、電文を送信する。不正操作を検知した場合にも正常な場合と同じ回数だけ電文のやりとりを続けて行う。また、偽電文は毎回異なるものにする。これにより、操作者に気づかれずに、不正操作による伝送エラーの場合には第1カウンタA、不正操作でも伝送エラーでも起こり得るエラー（不正操作の可能性がある）の場合には第2カウンタBをカウントアップしてカウンタ格納部514に蓄積することができる。

【0026】ICカード51の実行制御部512bは、また、端末41と通信を行うときに、カウンタ格納部514の蓄積情報を端末41のカウンタ格納部439に送信する機能を有する。これにより端末41では、図6に示すように、ICカード51側の電文番号に対応するカウンタ値A-n，B-nと同一のカウンタ値A'-n，B'-nをカウンタ格納部439に蓄積することができる。これにより、端末41において、ICカード51に対して行われた不正操作、ないし異常が発生した状況を知ることができ、必要な対策制御処理を行うことができる。これは、ICカード51を通じて端末41に不正アクセスを行おうとする者（以下、攻撃者）がどこまでアクセスに成功したかという情報を知ることができないうちに、端末41側で必要な対策を採り得ることを意味する。また、攻撃者にとって完全に不正アクセスを成功させることが著しく困難になることを意味する。

【0027】次に、上記ICカード51、端末41、サイト内制御装置31、およびホスト11を接続した場合のシステム運用例を具体的に説明する。

【0028】通常、端末41は、ICカード51が利用されたとき、上述のように、端末41のカウンタ格納部439内に、不正発生（不正操作）ないし不正発生の可能性がある状況を蓄積し、所定の時間帯や不正回数のうちはホスト11と通信し、情報交換を行う「集計処理モード」、すなわちオフラインで動作する。しかし、「不正の発生状況が異常」と判断した場合には、ホスト11とカードリーダライタ45とを接続して、ホスト11が直接ICカード51のチェックを行う「オンラインモード」に切り換える。また、利用されたカード51が不正（不正操作がある）、または利用状況が不正と判断された場合には利用の制限を行う。これらの制御処理は、端末41内の危機管理表433aに基づいて対策制御処理部432が自動実行する。

【0029】ここで用いる端末41の危機管理表433

aの一例を図7に示す。この危機管理表433aは、電子現金、プリペイド、電子小切手等の額面をデータとして、これらのデータを扱う情報通信システムを想定した場合の例である。ここでは、管理項目毎に管理限界値を持ち、管理限界値に対応して対策制御処理の内容が設定される。管理項目としては以下のようなものを設定する。

【0030】（データ利用間隔）データ利用間隔tを管理項目とする。システムの性質上、ある時間間隔を超えるように利用が考えられない場合、その時間間隔を管理限界値とする。この場合の対策制御処理部432が実行する内容としては、管理限界値を超える利用間隔であることを検知したとき、次のデータ利用を不可能にしてサービスを行わない、あるいは利用データ量に制限を加えるようにする。これにより、暗号化／復号化、認証などによって検知できなかった不正操作による損害を格段に低減させることができる。

【0031】（データID、カードID）データ毎にID情報が付されている場合、またはICカード51毎にID情報が付されている場合に、これらID情報を管理項目として設定する。対策制御処理部432は、特定のID情報が付されたデータやICカード51に正当なものと不正なものがあることが判っている場合、カードリーダライタ45に装着されたICカードを排出しないようにする。あるいは、不正なデータやICカード、取引、年月日に対する処理を再現しないようにする。これにより、システム運用の安全性が低下することを防ぐことができる。

【0032】（センタと通信不可（オフライン）時のデータ利用量）センタ（ホスト11）との通信不可時に利用されるデータ量cを管理項目とする。センタでのみ検出できる不正や移動動作がある場合に設定する。通常は無条件で利用可能とする。対策制御処理部432は、この値が、ある値（c＝1，000）以上では当日に同じサイトで発行・提供されたデータのように、信頼性の高いデータのみ利用できるようし、より厳しい値（c＝10，000）以上になった場合にはデータ利用動作を停止させる。これにより、オフライン時に検出できない不正操作による損害を低減することができる。

【0033】（不正検知カウンタ、不正らしさ検知カウンタ）ICカード51や端末41の不正検知カウンタ（第1カウンタA）、不正らしさカウンタ（第2カウンタB）をそれぞれ管理項目とする。通常は無条件で利用可能とする。対策制御処理部432は、カウンタ値が各管理限界値以上の場合、管理限界値の大きさに対応した対策制御処理を行う。つまり、管理限界値が厳しくなるに応じて、使用履歴管理と利用制限を厳しくする。この場合の対策制御処理の具体例として以下のようなものが挙げられる。

（1）端末41内にIDとカウンタ値を蓄積するとともに、蓄積情報を一定のタイミングでサイト内制御装置31に送信する。

（2）ICカード51の利用時にサイト内制御装置31に所要データを送信する。

（3）操作者が利用できるサービスを制限する。

（4）ICカード51をロックし、ホスト11にカードIDを送信する。

これにより不正状況の情報を上位装置に必要最低限だけ送ることができ、通信量の節減を図ることができる。

【0034】（カードマスタ検索時のデータ利用量）ICカード51を電子財布として使用し、その利用残高や管理情報を含むカードマスタ情報を同サイトや他サイトのサイト内制御装置から検索する場合、検索を行っている時間内のデータ利用量を管理項目とする。対策制御処理部432は、データ利用量が管理限界値以上の場合、そのカードアクセスを停止させる。これにより、カードマスタ情報を参照する時間が長い場合でも、不正による損害を一定に抑えて、サービスを停止せずに運用することができる。

【0035】対策制御処理部432が行う上記処理の概略的な流れを図8に示す。動作間隔を管理項目としている場合は、動作を行う前に時間計測部441で計測した時刻を読み出し（S21）、前の処理との動作間隔を算出する（S22）。続いて、通信ないしカードアクセスを行った後（S23）、集計処理モード（オフライン）か否かを判断する（S24）。集計処理モードの場合（S24：Yes）は、装置内の危機管理表433aに従って処理を行う。集計処理モードでない場合（S24：No）にはオンラインモードで動作し、ホスト11の指示に従って処理を行う。

【0036】集計処理モードの場合は、管理項目kに1を代入し（S25）、計測値・統計値Ckの収集・算出を行う（S26）。次に、限界値の数iを設定し（S27）、上記Ckの値と管理限界値Lkiとを比較する（S28）。Ck＜Lkiならば、iが1か否かを判断し（S29）、i＝1ならば、kの値が管理項目数kに等しいか否かを判断する（S30）。等しければそのモードの処理を終了する。一方、S28の処理において、Ck≧Lkiならば、対策（ki）を実行し（S31）、S29の処理において、i＝1でなければi＝i－1として（S32）、S28の処理に戻る。S30において、kが管理項目数kに達していない場合は、k＝k＋1として（S33）、S26の処理に戻る。

【0037】すなわち、集計処理モードでは、通信動作あるいはカードアクセスによって得られた情報や前の処理との時間間隔等から、各管理項目に従って「統計値・計測値」を算出する。次に「統計値・計測値」を管理限界値と比較し、「管理限界値」以上の場合には対応する「対策制御処理」を行う。複数の管理限界値がある場合には、条件を満たす最も厳しい管理限界値に対応する

「対策制御処理」を行う。全ての管理項目に対し管理限界値との比較を行い、そのモードを終了する。

【００３８】一方、オンラインモードの場合は、ホスト１１にカードアクセスにより得た情報を送信する（Ｓ３４）。そして、ホスト１１からの返信情報を受信し（Ｓ３５）、その返信情報に含まれる指示に従ってサービス実施や動作停止等の処理を実行して（Ｓ３６）、そのモードを終了する。

【００３９】このように、端末４１に危機管理表４３３ａを備えることで不正操作ないし不正操作の可能性がある場合に、端末４１が、主導的に、あるいはホスト１１からの指示を受けて直ちに必要な対策制御処理を施すことが可能になる。また、端末４１における現在の監視情報、例えばカウンタ格納部４３９に蓄積されている情報等をホスト１１が随時収集することで、システム全体の安全性がどこまで低下したかを知ることができ、システム更新の時期や次の対策の指標を得ることができる。また、収集した監視情報に基づき危機管理表４３３ａの内容を随時更新することで、不正操作に基づくサービス実施その他の処理を未然に防止することができ、安全にシステムを維持することができる。

【００４０】なお、以上は、危機管理表を端末４１に備えた場合の例であるが、ホスト１１、サイト内制御装置３１、端末４１に各々自端末固有の危機管理表を持たせることが好ましい。特に、システムが階層構造の場合、各階層毎に危機管理表を備えることが好ましい。

【００４１】図９に、ホスト１１－サイト内制御装置３１－端末４１の３階層に、各目的に応じた危機管理表を備える例を示す。この場合、ホスト１１およびサイト内制御装置３１は、端末４１における対策制御処理部４３２と同様のデータ処理手段を備えている。

【００４２】ホスト用危機管理表は、例えば、通信不可時の処理・対策、サイト間の使用データの管理、システム全体のデータ量の把握・管理（出力－入力）、システム全体の不正状況の管理、管理者への通知管理を目的とする。サイト内制御装置用危機管理表は、例えば、通信不可時の処理・対策、サイト内でのデータ量の管理・把握（出力－入力）、入出力の傾向管理、サイト内の不正状況の管理、センタへの通知管理を目的とする。端末用危機管理表は、図７に示したような管理項目、対策・処理を設定する。

【００４３】このような目的で備えられるサイト内制御装置３１内の危機管理表では、ホスト１１との通信不可時に利用されたデータの量や、通常時のサイト内のデータ量、不正の傾向が管理項目となる。通常時のサイト内のデータ量としては、下記計算式に示される、発行・提供したデータ（出力データ）と利用されたデータ（入力データ）の差・割合や、利用されたデータにおける「他サイトで発行・提供したデータ」の量・割合が管理される。この場合の対策制御処理としては、ホスト１１への通知や、利用データの制限、利用可能な装置の制限が挙げられる。

（計算式）

＜出力データと入力データの差＞＝（出力データ）－（入力データ）

＜出力データと入力データの割合＞＝（出力データ）／（入力データ）

＜他サイト発行・提供データの割合＞＝（他サイト出力データ）／（入力データ）

【００４４】ホスト１１内の危機管理表では、サイト間のデータの移動量や、システム全体における出力データと入力データの差・割合、不正発生回数、サイト内制御装置３１との通信不可時の不正発生回数、通信不正時間が管理項目となる。この場合の対策制御処理としては、管理者への通知、利用データの制限、サイト内制御装置３１や端末４１内の危機管理表の更新等が挙げられる。

【００４５】このように、本実施形態の情報通信システムでは、暗号方法の変更等のシステム更新時期の指標を容易且つ少ない負荷で得ることができる。しかも、高いセキュリティを維持できることから、電子現金等の財貨を扱うシステムを安全に構築することができる。また、大規模なシステムで細かな危機管理を行いたい場合に、該危機管理に必要な負荷を分散させ、利用に要する時間を短縮できる点で有効となる。

【００４６】

【発明の効果】以上詳述したように、本発明によれば、オフラインでＩＣカードに不正操作がなされた場合であっても、それを利用する情報処理端末あるいは上位装置で不正操作の状況を確実に収集することができる効果がある。また、不正操作を検知した場合には、ＩＣカードが攻撃者が判らないような偽電文を送るため、複数の電文をやりとりする処理では、攻撃者に対して必要な情報を与えることがない。よって、全ての暗号鍵や認証処理の手順を完全に知られない限り、セキュリティを破られにくく、高いセキュリティを確保できる効果がある。

【００４７】さらに、不正操作と断定できない異常動作については、監視情報に基づいて詳細な状況を得ることができ、不正操作や不正操作らしい動作の検知・対策制御処理によるセンタの負荷も少なく、不正操作と断定できない不正操作が発生した場合にも、損害を抑えることができる効果がある。

【００４８】加えて、必要時だけオンラインチェックに切り換わるようにすることができるため、安全性を高めた場合にも回線使用のコストを削減できる効果がある。また、回線の不具合でホスト等と通信できなくなった場合に、情報処理端末を動作させ続けても、不正に基づく損害を抑えることができる。

【００４９】さらに、危機管理表の内容を運用中に動的に更新することにより、システム設計時に予測されなかった不正状況が発生しても、それに起因する損害を削減

できるという効果がある。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る情報通信システムの全体構成を示すブロック図。

【図2】この実施形態による端末の詳細ブロック構成図。

【図3】この実施形態によるＩＣカードの内部ブロック構成図。

【図4】ＩＣカードにおける、不正ないし不正らしき電文の検知・対策・発生状況の収集の手順を示すフローチャート。

【図5】ＩＣカードに不正検知機能をもたせる場合の、端末間の電文の流れを示す図。

【図6】端末とＩＣカードに備えられるカウンタ格納部の関係説明図。

【図7】この実施形態における危機管理表の一例を示す説明図。

【図8】危機管理表を用いた端末装置での対策制御処理の手順説明図。

【図9】ホスト－サイト内制御装置－端末の３階層に危機管理表を備えた情報通信システムの接続状態説明図。

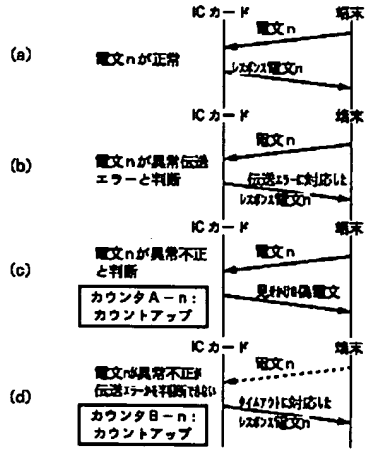
【符号の説明】

11　ホストコンピュータ
111　端末監視処理装置
112　オンライン処理装置
113　危機管理表格納部

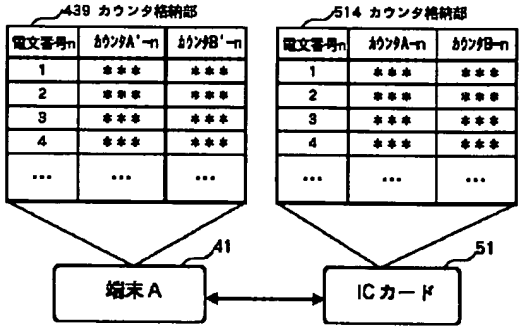


113a　ホストの危機管理表
21　通信回線
31　サイト内制御装置
41　端末（情報処理端末）
43　主制御装置
431　主制御部
432　対策制御処理部
433　危機管理表格納部
433a　危機管理表
434　デバイス管理部
435　通信制御部
436　カード制御部
437　警報制御部
438　カウンタ処理部
439　カウンタ格納部
440　不正検知部
441　時間計測部
51　ＩＣカード
512　ＩＣカードのＣＰＵ
512b　実行制御部
513　ＩＣカードのＲＯＭ
513b　カウンタ処理部
514　ＩＣカードのＥＥＰＲＯＭ内に構成されるカウンタ格納部
515　ＩＣカードのＲＡＭ

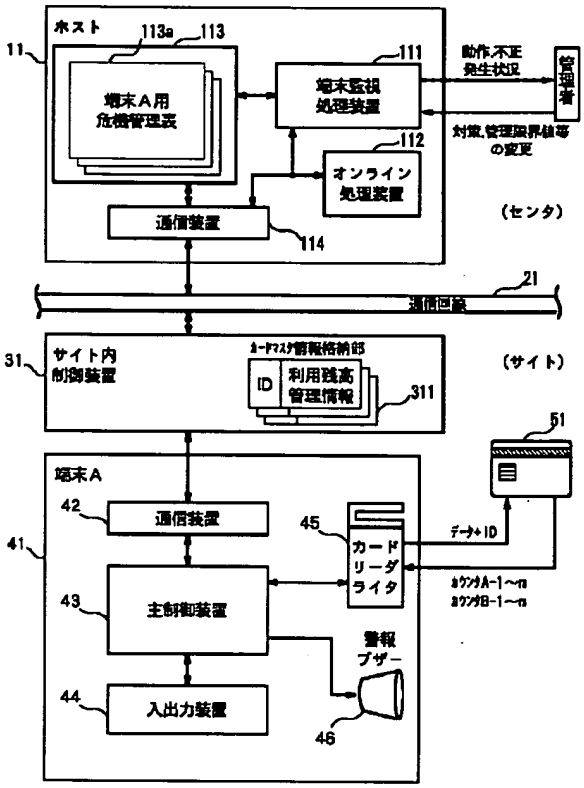
【図5】



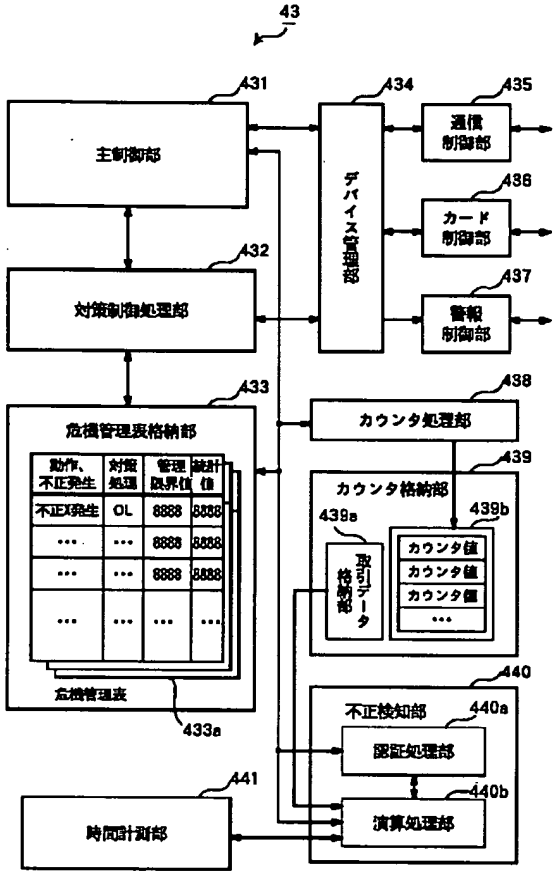

【図6】



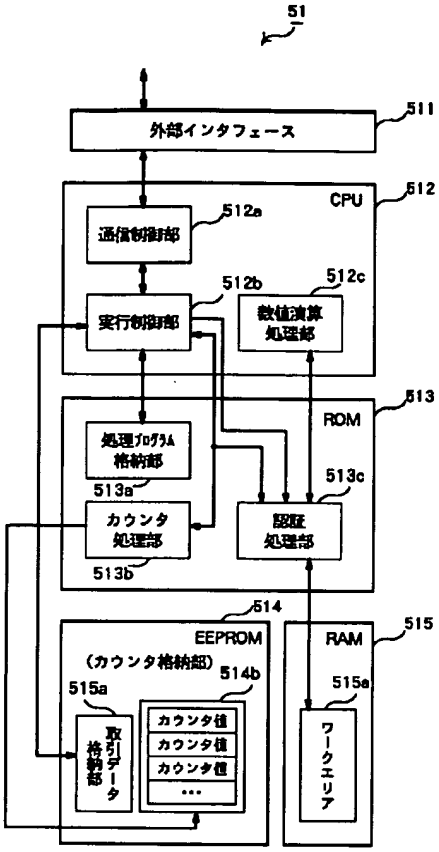
【図1】


ホスト
11
113a
113
端末A用
危機管理表
111
端末監視
処理装置
動作,不正
発生状況
管理者
対策,管理限界値等
の変更
112
オンライン
処理装置
通信装置
114
（センタ）
21
通信回線
31
サイト内
制御装置
ユーザ情報格納部
ID
利用残高
管理情報
311
（サイト）
51
端末A
42
通信装置
45
カード
リーダ
ライタ
データ+ID
カウンタA-1～n
カウンタB-1～n
41
43
主制御装置
警報
ブザー
44
入出力装置
46

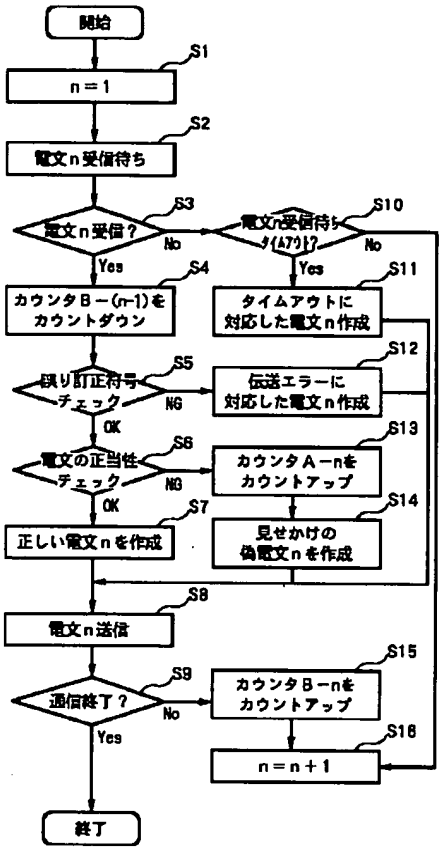
【図2】


43
431
主制御部
434
デバイス管理部
435
通信
制御部
436
カード
制御部
437
警報
制御部
432
対策制御処理部
433
危機管理表格納部
動作、
不正発生
対策
処理
管理
限界値
統計
値
不正発生
OL
8888
危機管理表
433a
438
カウンタ処理部
439
カウンタ格納部
439a
取引データ
格納部
439b
カウンタ値
カウンタ値
カウンタ値
440
不正検知部
440a
認証処理部
440b
演算処理部
441
時間計測部

【図3】


51
外部インタフェース
511
CPU
512
通信制御部
512a
実行制御部
512b
数値演算処理部
512c
ROM
513
処理プログラム格納部
513a
カウンタ処理部
513b
認証処理部
513c
EEPROM
514
(カウンタ格納部)
514b
取引データ格納部
515a
カウンタ値
カウンタ値
カウンタ値
...
RAM
515
515a
ワークエリア

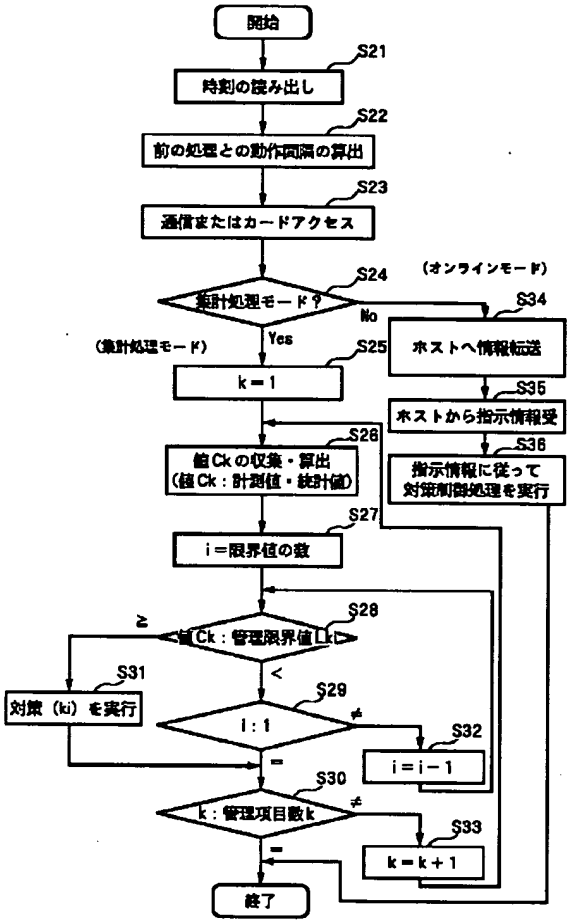
【図4】


開始
S1
n＝1
S2
電文n受信待ち
S3
電文n受信？
No
Yes
S10
電文n受信待ちタイムアウト？
No
Yes
S4
カウンタB－(n-1)をカウントダウン
S11
タイムアウトに対応した電文n作成
S12
伝送エラーに対応した電文n作成
S5
誤り訂正符号チェック
NG
OK
S6
電文の正当性チェック
NG
OK
S13
カウンタA－nをカウントアップ
S14
見せかけの偽電文nを作成
S7
正しい電文nを作成
S8
電文n送信
S9
通信終了？
No
Yes
S15
カウンタB－nをカウントアップ
S16
n＝n＋1
終了

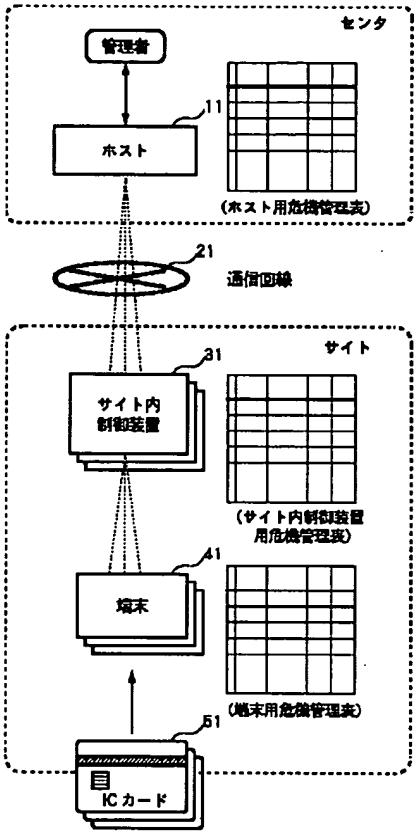
【図7】

| 項番 | 管理項目 | 対策制御処理 | 管理限界値 | 限界値の数 | 統計・計測値 |
|---|---|---|---|---|---|
| 1 | 10回のデータ利用間隔1秒 | 次回以降のサービスを行わない | t=100 | 1 | t=## |
| 2 | PIN不一致がn回 | カードをロックし、カードIDをセンタに通知する | n=6 | 1 | n=## |
| 3 | データIDが不正 | カードを排出しない | ID=13456, 13783, | n | ID=## |
| 4 | センタと通信不可（オフライン）時のデータ利用量C | 当日、当サイト内での発行・受信データのみ利用可能 | C=1,000 | 2 | C=## |
| | | 動作停止 | C=10,000 | | |
| 5 | カード側不正検知カウンタA1 | サイト内制御装置に通知 | A1=1 | 3 | A1=## |
| | | サービス利用時制限を行う | A1=127 | | |
| | | カードをロックし、カードIDをセンタに通知する | A1=255 | | |
| 6 | カード側不正らしき検知カウンタB1 | 端末内にID、カウンタ値等を蓄積 | B1=1 | 3 | B1=## |
| | | サイト内制御装置に通知 | B1=127 | | |
| | | サービス利用時制限を行う | B1=255 | | |
| 7 | 端末側不正検知カウンタA'1 | | | 3 | A'1=## |
| 8 | 端末側不正らしき検知カウンタB'1 | | | 3 | B'1=## |
| 9 | カード側不正検知カウンタA2 | | | 3 | A2=## |
| 10 | カード側不正らしき検知カウンタB2 | | | 3 | B2=## |
| 11 | 端末側不正検知カウンタA'1 | | | 3 | A'2=## |
| 12 | 端末側不正らしき検知カウンタB'2 | | | 3 | B'2=## |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| ** | カード側不正らしき検知カウンタBn | 完全オフラインモードに移行 | Bn=255 | 3 | Bn=## |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| ** | カードマスタ検索中のデータ利用量C' | 動作停止 | C'=1,000 | 1 | C'=## |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

【図8】



【図9】




---

フロントページの続き

(72)発明者　加藤　公博
東京都江東区豊洲三丁目３番３号　エヌ・
ティ・ティ・データ通信株式会社内